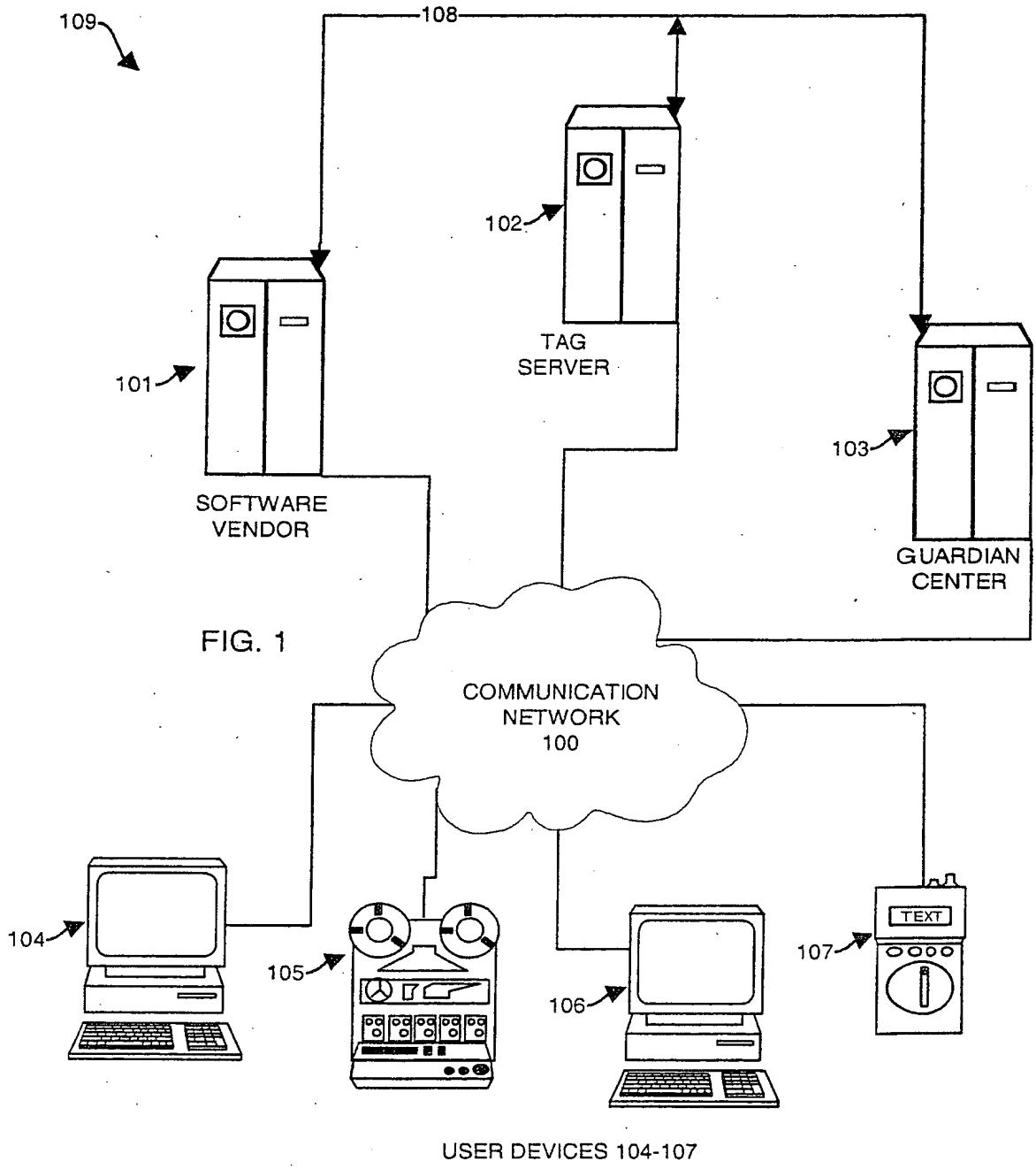

109
108
102
TAG
SERVER
101
SOFTWARE
VENDOR
103
GUARDIAN
CENTER
COMMUNICATION
NETWORK
100
104
105
106
107
TEXT
USER DEVICES 104-107

FIG. 1

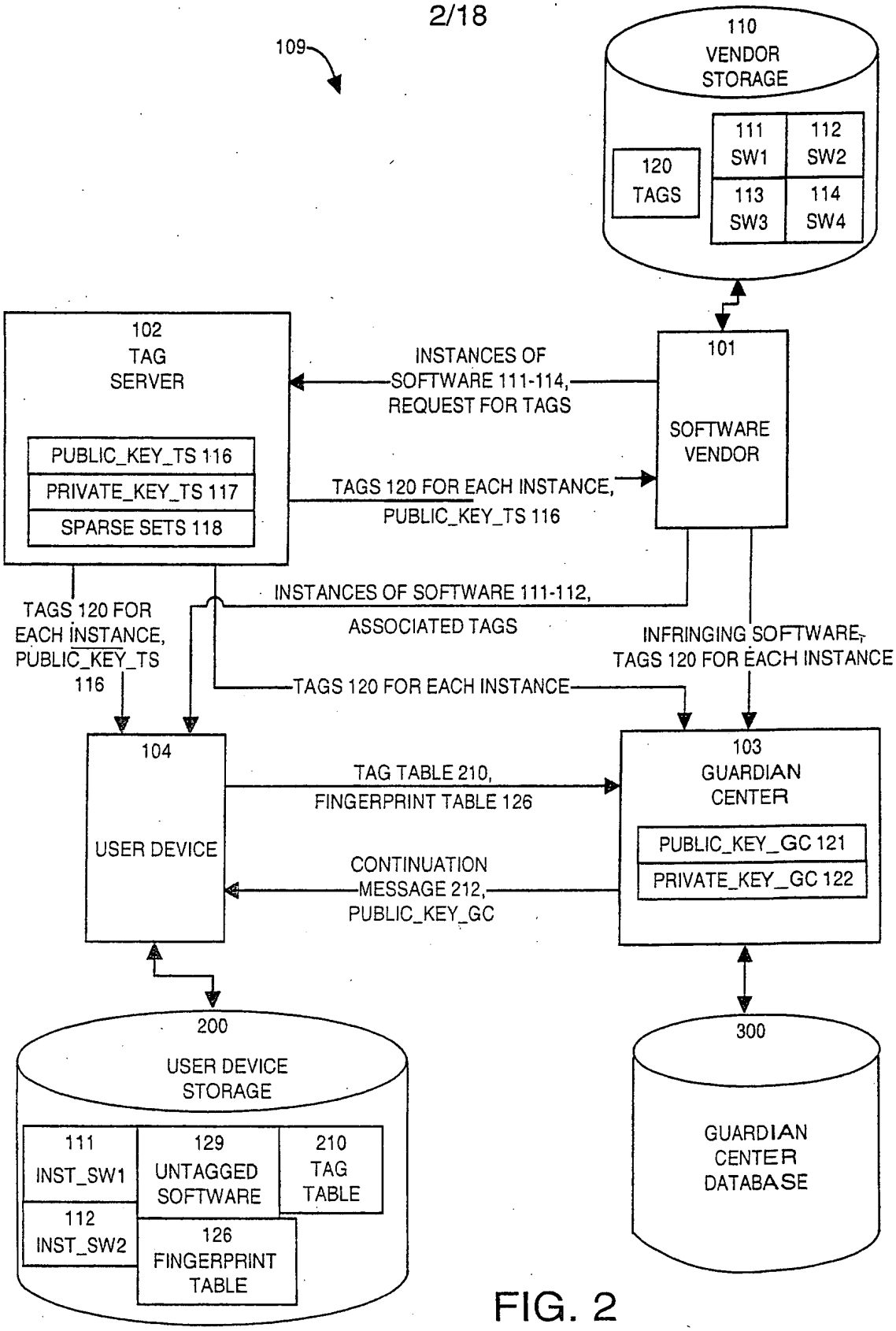
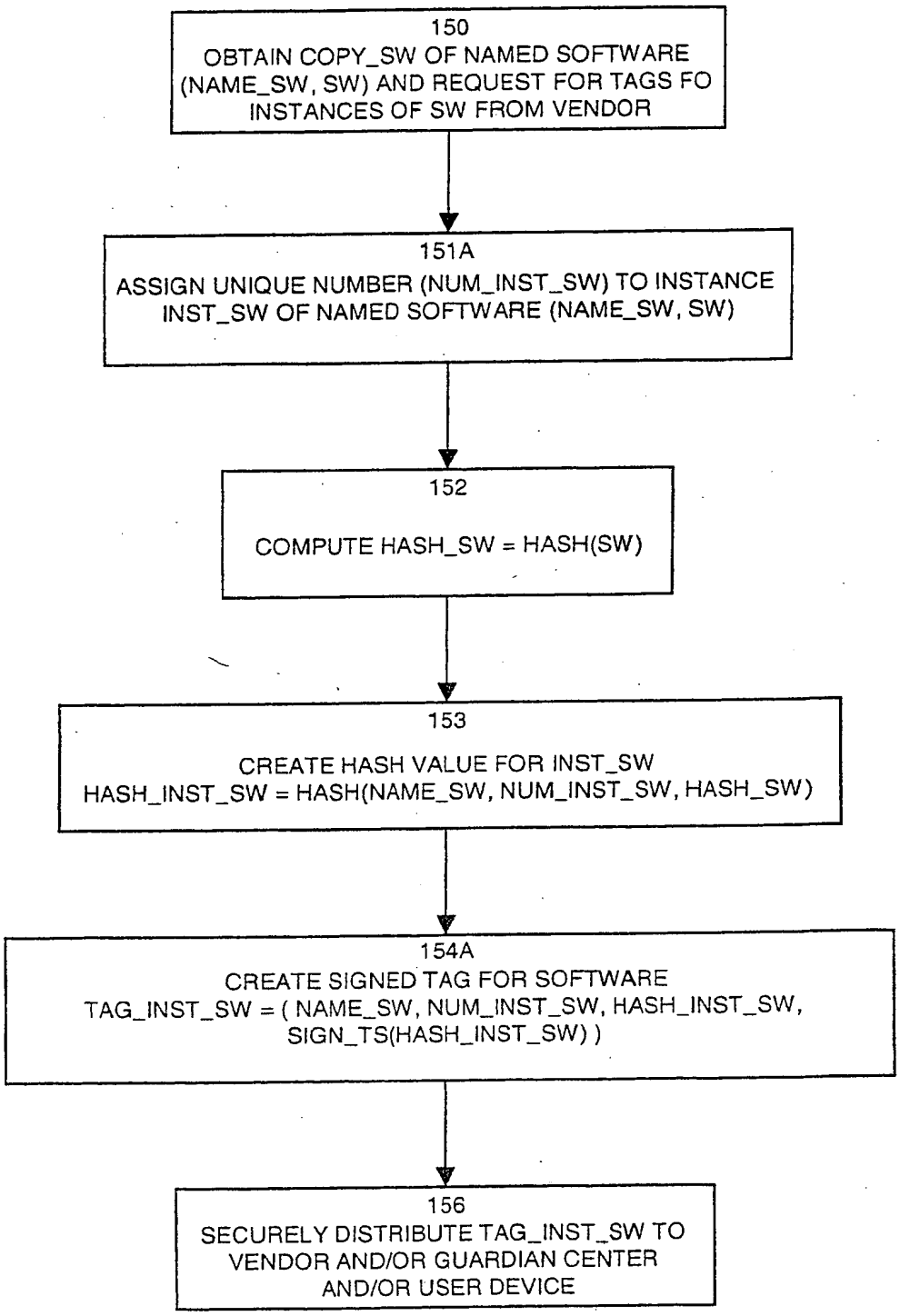
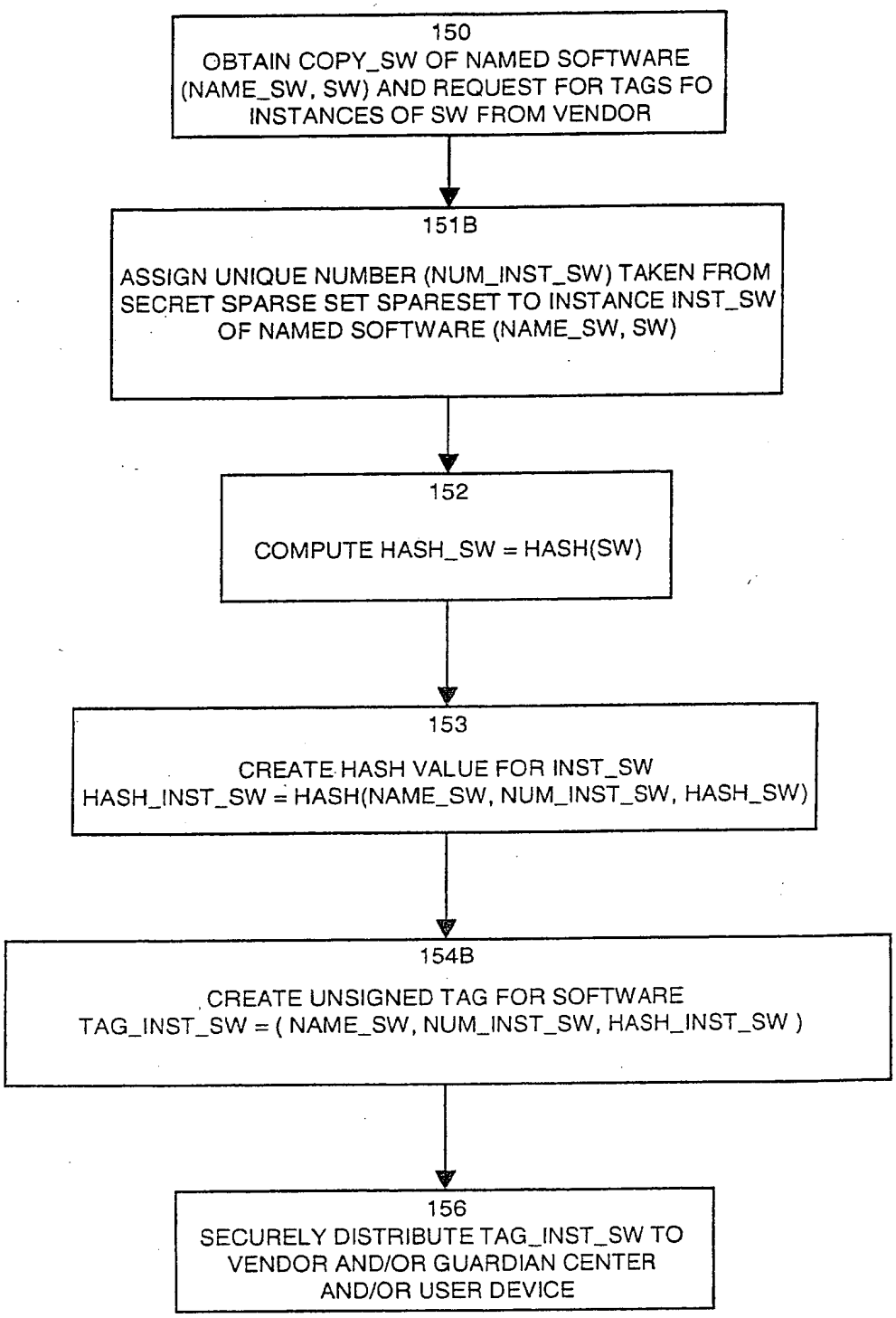

109
110
VENDOR
STORAGE
111
SW1
112
SW2
113
SW3
114
SW4
120
TAGS
102
TAG
SERVER
PUBLIC_KEY_TS 116
PRIVATE_KEY_TS 117
SPARSE SETS 118
INSTANCES OF
SOFTWARE 111-114,
REQUEST FOR TAGS
101
SOFTWARE
VENDOR
TAGS 120 FOR EACH INSTANCE,
PUBLIC_KEY_TS 116
INSTANCES OF SOFTWARE 111-112,
ASSOCIATED TAGS
TAGS 120 FOR
EACH INSTANCE,
PUBLIC_KEY_TS
116
INFRINGING SOFTWARE,
TAGS 120 FOR EACH INSTANCE
TAGS 120 FOR EACH INSTANCE
104
USER DEVICE
TAG TABLE 210,
FINGERPRINT TABLE 126
103
GUARDIAN
CENTER
PUBLIC_KEY_GC 121
PRIVATE_KEY_GC 122
CONTINUATION
MESSAGE 212,
PUBLIC_KEY_GC
200
USER DEVICE
STORAGE
111
INST_SW1
129
UNTAGGED
SOFTWARE
210
TAG
TABLE
112
INST_SW2
126
FINGERPRINT
TABLE
300
GUARDIAN
CENTER
DATABASE

FIG. 2



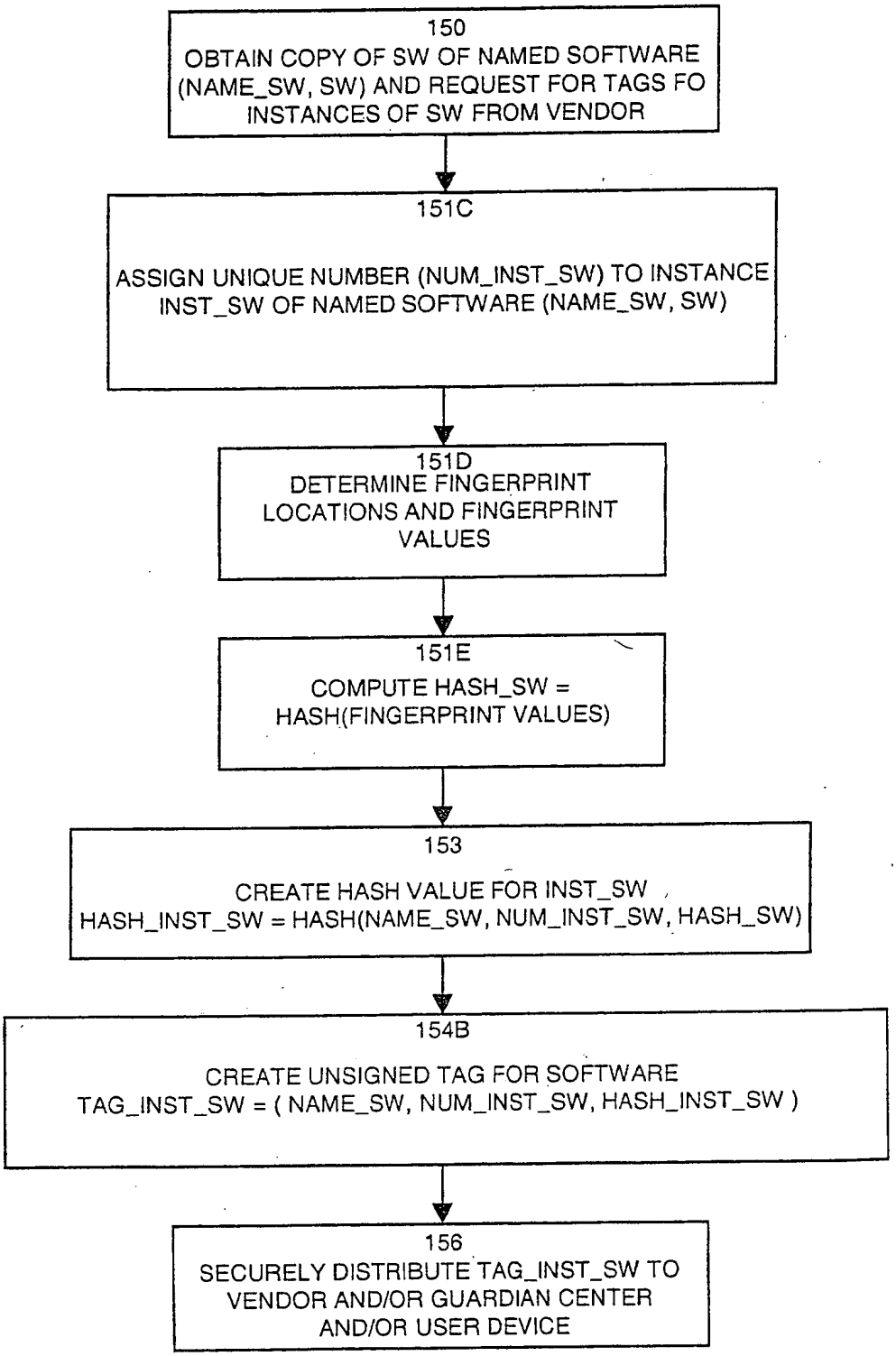
SIGNED TAG CREATION BY TAG SERVER

FIG. 3A



UNSIGNED TAG CREATION BY TAG SERVER

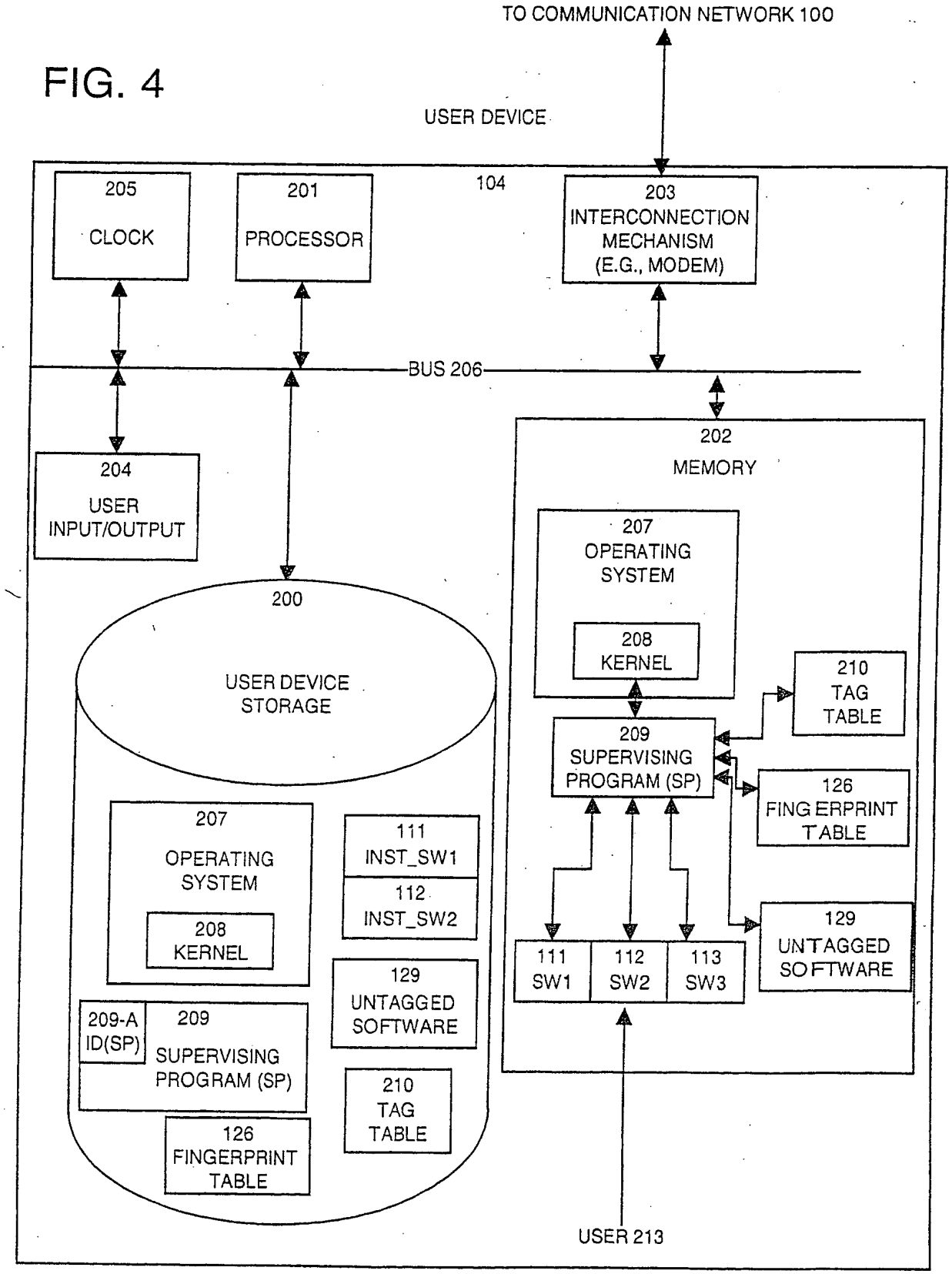
FIG. 3B

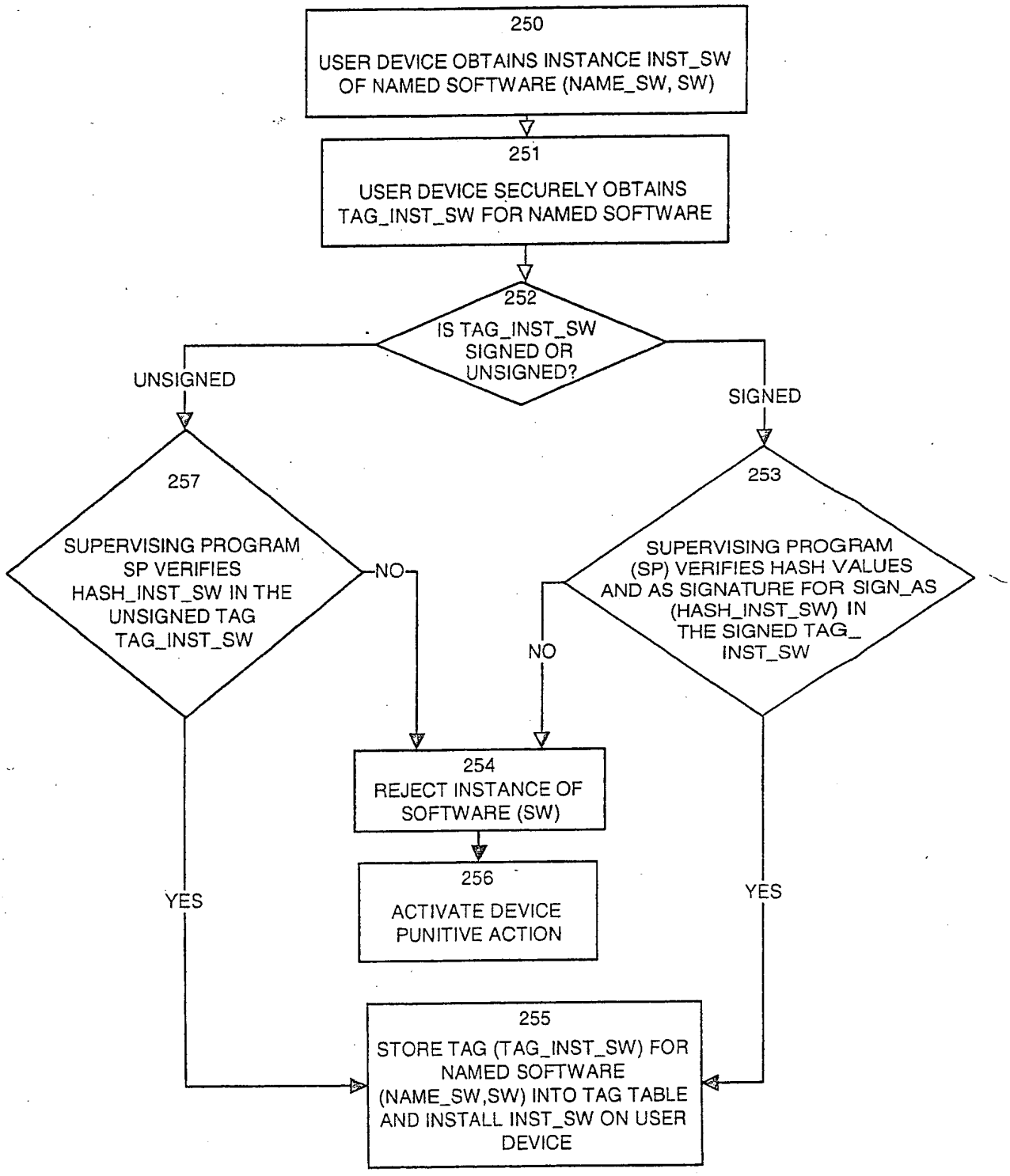


TAG CREATION USING SAME LOCATION FINGERPRINTING BY TAG SERVER

FIG. 3C

FIG. 4


TO COMMUNICATION NETWORK 100
USER DEVICE
104
205
CLOCK
201
PROCESSOR
203
INTERCONNECTION MECHANISM (E.G., MODEM)
BUS 206
202
MEMORY
204
USER INPUT/OUTPUT
200
USER DEVICE STORAGE
207
OPERATING SYSTEM
208
KERNEL
210
TAG TABLE
209
SUPERVISING PROGRAM (SP)
126
FINGERPRINT TABLE
207
OPERATING SYSTEM
208
KERNEL
111
INST_SW1
112
INST_SW2
129
UNTAGGED SOFTWARE
209-A
ID(SP)
209
SUPERVISING PROGRAM (SP)
210
TAG TABLE
126
FINGERPRINT TABLE
111
SW1
112
SW2
113
SW3
129
UNTAGGED SOFTWARE
USER 213



INSTALLING TAGGED INSTANCE OF VENDOR SOFTWARE (SW) ON USER DEVICE

FIG. 5

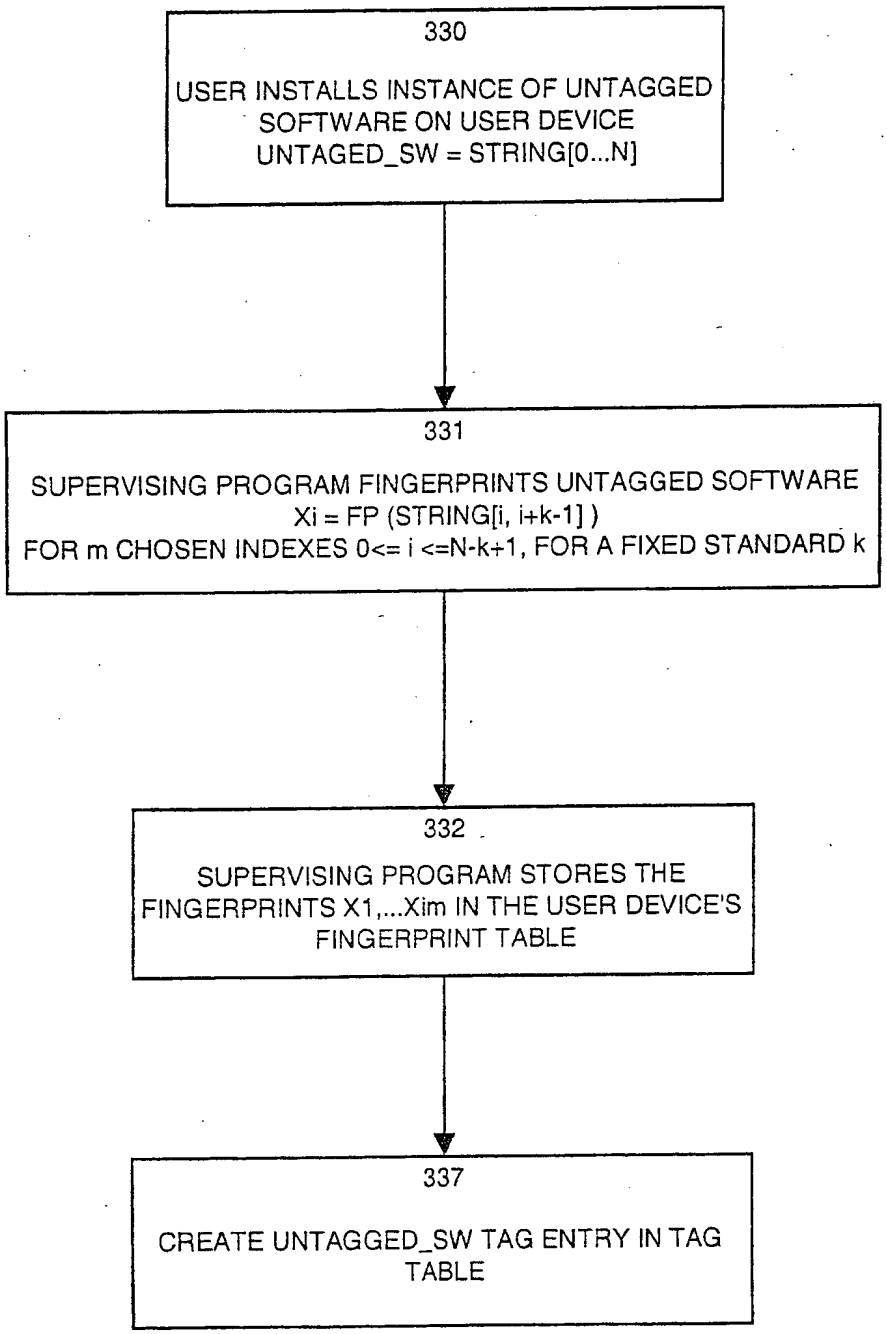
TAG TABLE

210				
HEADER_TAG_TABLE=(ID_TAG_TABLE, LAST_GC_CM, LAST_CALLUP_TIME, NUMBER_DEVICE_BOOTUPS)				
TAGS	USAGE STATUS	ACTION TIME	RUN COUNT	USE TIME
TAG_INST_SW1	CONTINUED	11/22/98 11:02	10	00:58
TAG_INST_SW2	INSTALLED REMOVED	11/24/98 21:36 11/26/98 09:31	3	00:11
TAG_INST_SW3	GC_DISABLED	11/22/98 11:02	0	00:00
TAG_INST_SW4	CONTINUED	11/25/98 14:17	4	10:34
UNTAGGED_SW1	UNTAGGED	11/25/98 14:17	0	00:00

NOTE: ID_TAG_TABLE = (ID(USER)*, ID(DEVICE)*, ID(PP)*, ID(OS)*)

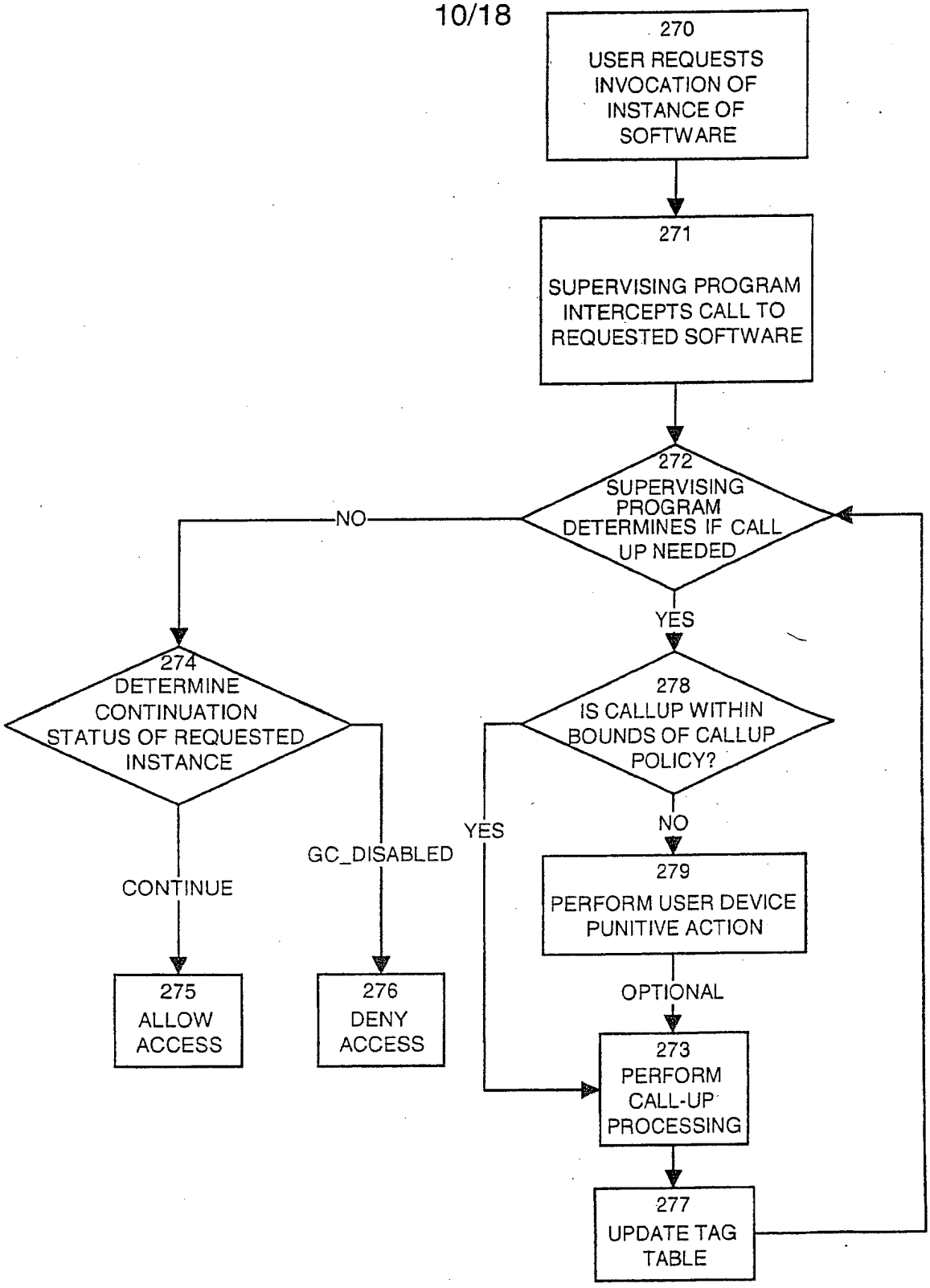
* MAY OR MAY NOT BE AVAILABLE

FIG. 6



INSTALLING UNTAGGED SOFTWARE (UNTAGGED_SW) ON USER DEVICE

FIG. 7



USAGE SUPERVISION PROCESSING

FIG. 8

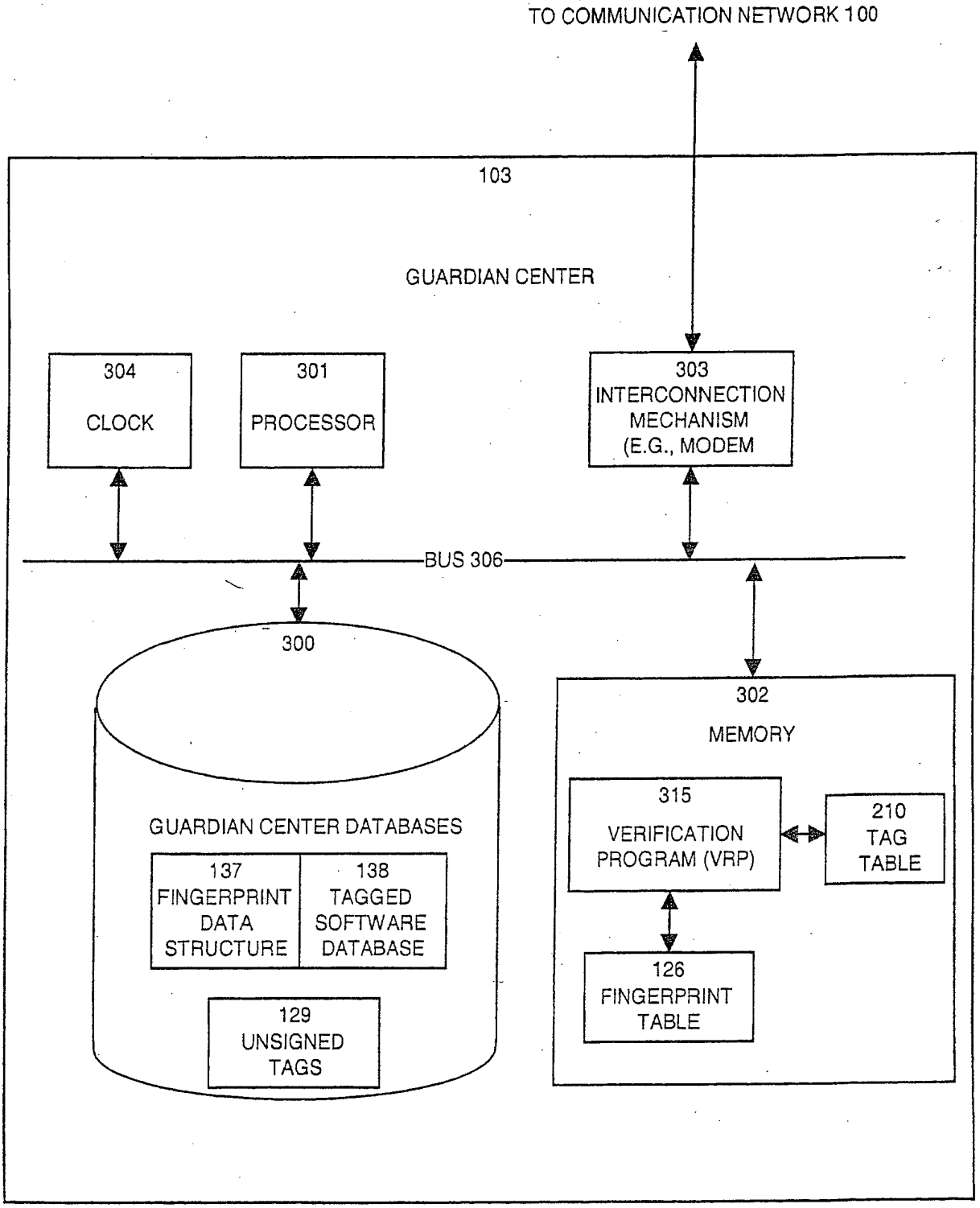

TO COMMUNICATION NETWORK 100
103
GUARDIAN CENTER
304
CLOCK
301
PROCESSOR
303
INTERCONNECTION MECHANISM (E.G., MODEM
BUS 306
300
GUARDIAN CENTER DATABASES
137
FINGERPRINT DATA STRUCTURE
138
TAGGED SOFTWARE DATABASE
129
UNSIGNED TAGS
302
MEMORY
315
VERIFICATION PROGRAM (VRP)
210
TAG TABLE
126
FINGERPRINT TABLE

FIG. 9

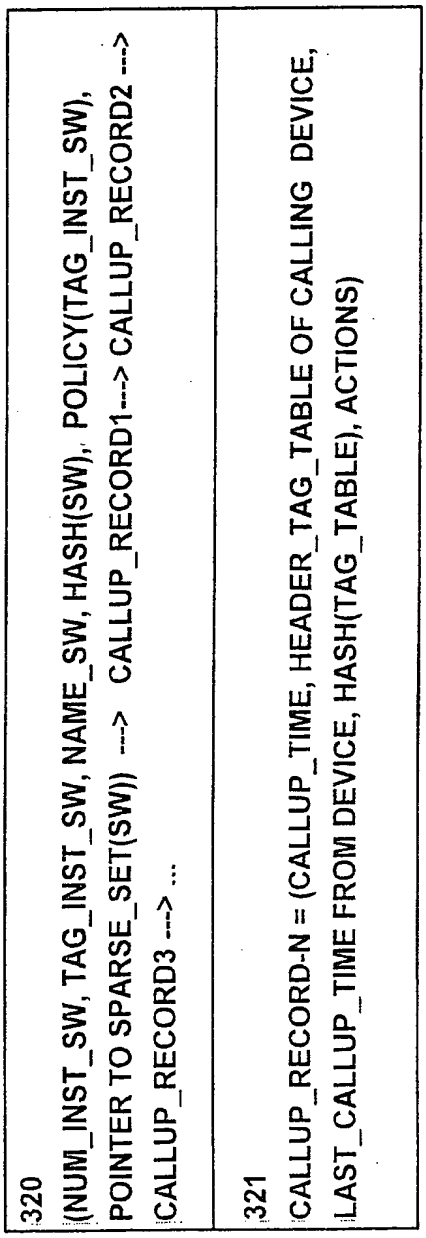

320
(NUM_INST_SW, TAG_INST_SW, NAME_SW, HASH(SW), POLICY(TAG_INST_SW),
POINTER TO SPARSE_SET(SW)) ---> CALLUP_RECORD1---> CALLUP_RECORD2 --->
CALLUP_RECORD3 ---> ...
321
CALLUP_RECORD-N = (CALLUP_TIME, HEADER_TAG_TABLE OF CALLING DEVICE,
LAST_CALLUP_TIME FROM DEVICE, HASH(TAG_TABLE), ACTIONS)
GUARDIAN CENTER DATA

FIG. 10

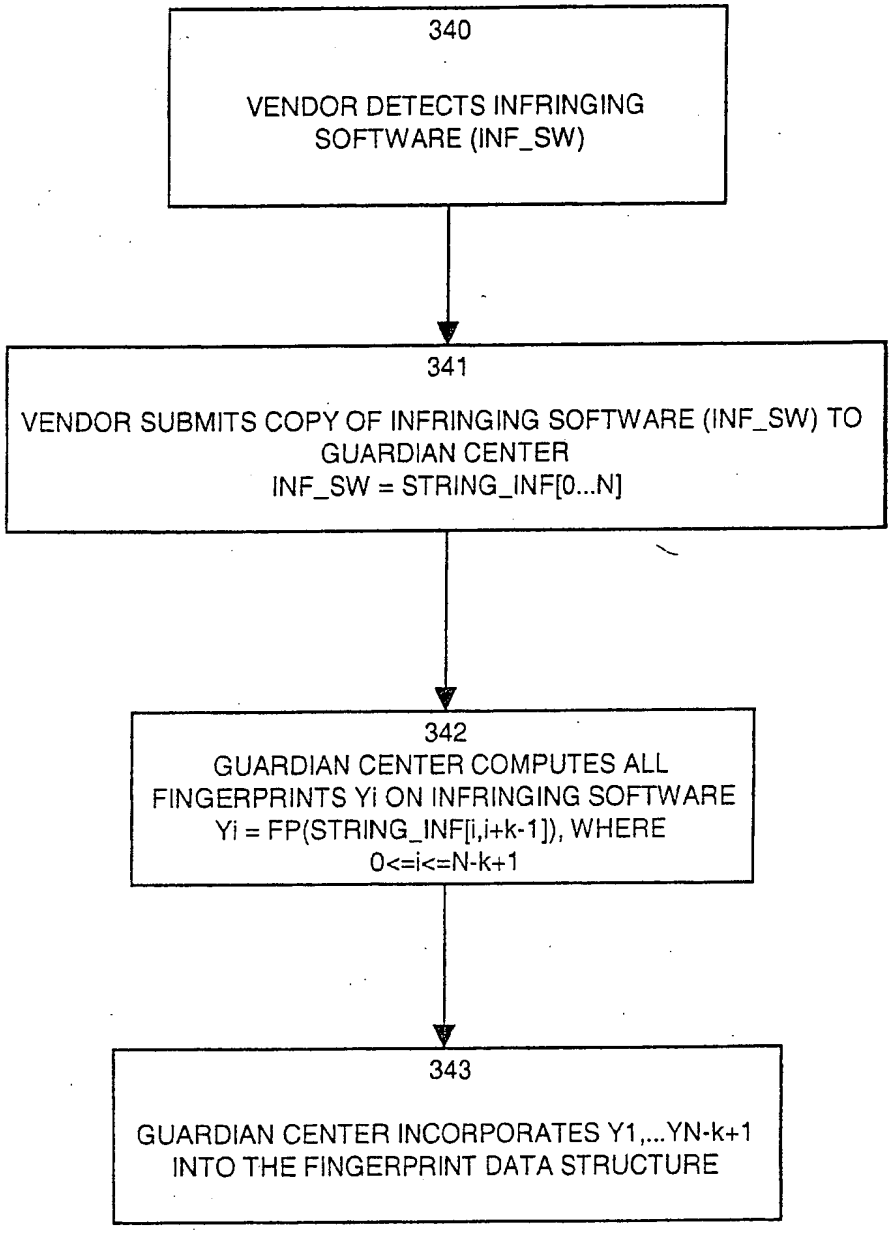

340
VENDOR DETECTS INFRINGING SOFTWARE (INF_SW)
341
VENDOR SUBMITS COPY OF INFRINGING SOFTWARE (INF_SW) TO GUARDIAN CENTER
INF_SW = STRING_INF[0...N]
342
GUARDIAN CENTER COMPUTES ALL FINGERPRINTS Yi ON INFRINGING SOFTWARE
Yi = FP(STRING_INF[i,i+k-1]), WHERE
0<=i<=N-k+1
343
GUARDIAN CENTER INCORPORATES Y1,...YN-k+1 INTO THE FINGERPRINT DATA STRUCTURE
GUARDIAN CENTER MADE AWARE OF INFRINGING SOFTWARE

FIG. 11

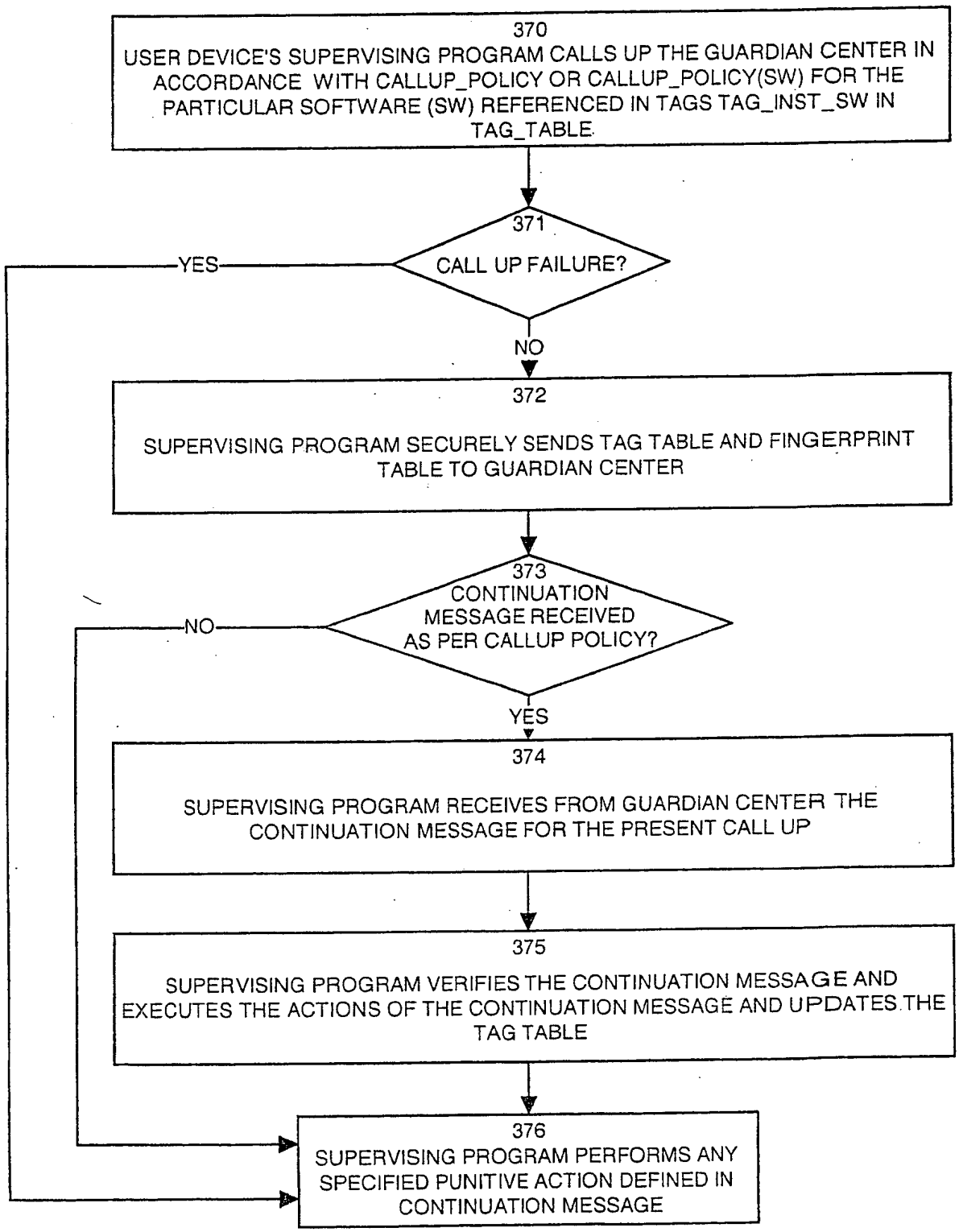
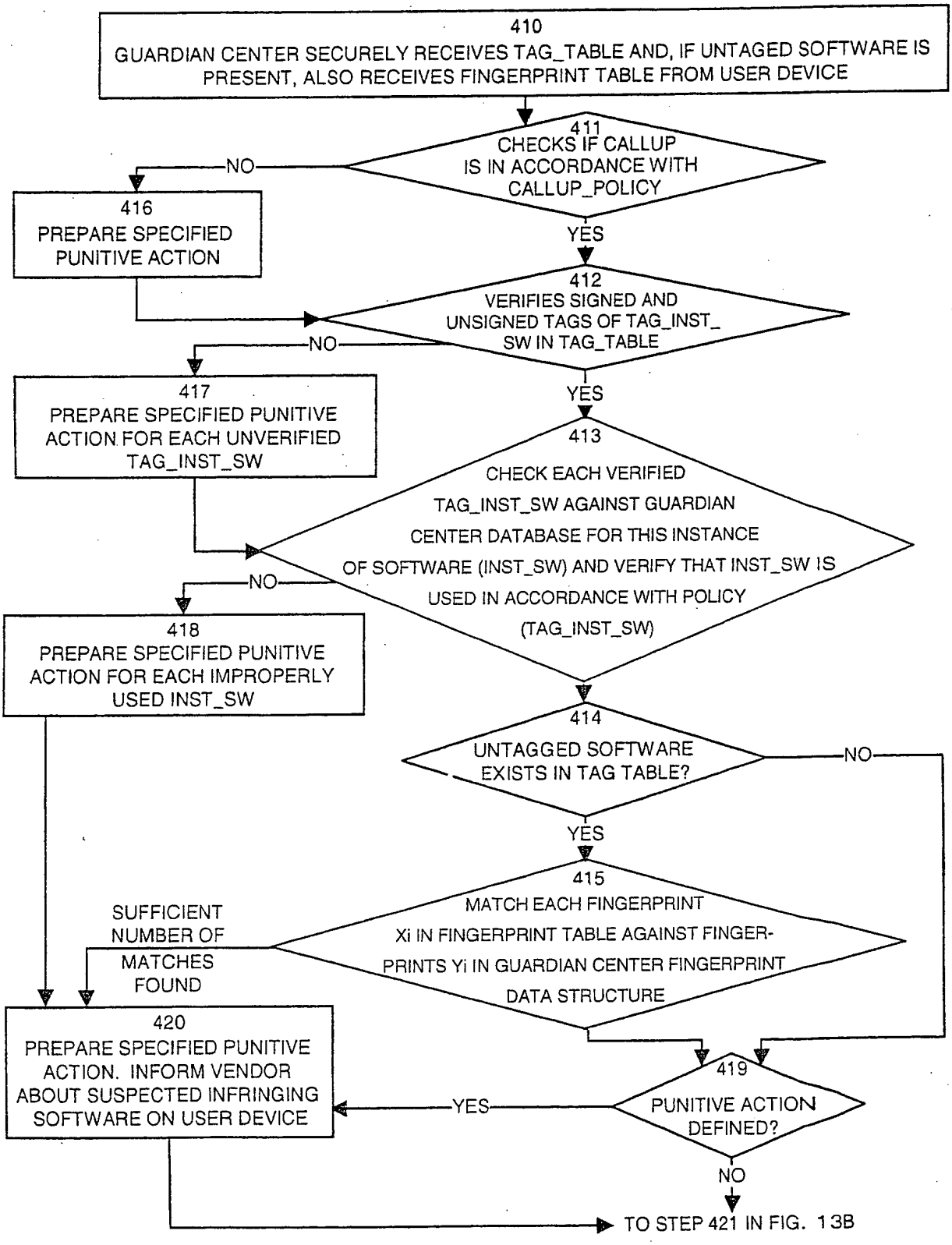
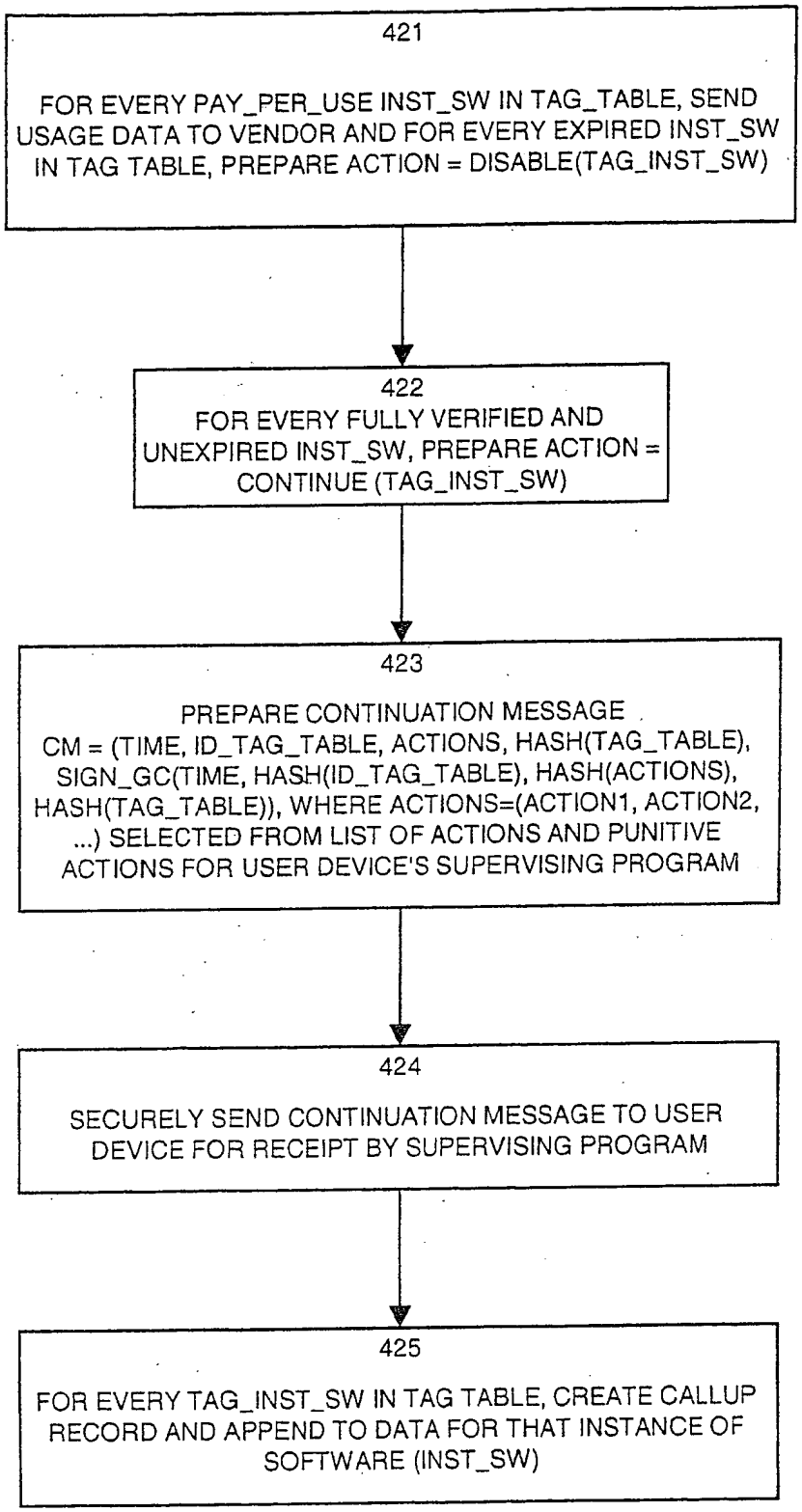


FIG. 12 CALL UP OF GUARDIAN CENTER FROM USER DEVICE



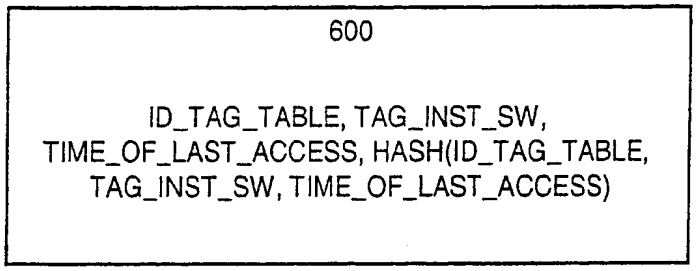
GUARDIAN CENTER CALLUP PROCESSING

FIG. 13A



GUARDIAN CENTER CALLUP PROCESSING

FIG. 13B



DATA TRANSFERRED WITH SHARED SOFTWARE DATA

601

TAG	ACCESS TIMES
TAG_INST_SW1	FEBRUARY 2, 1999 09:11 AM, DECEMBER 2, 1999 07:24 AM, FEBRUARY 1, 1999 09:36 PM, FEBRUARY 2, 1999 011:17 AM...
TAG_INST_SW2	JANUARY 5, 1999 10:19 PM, FEBRUARY 8, 1999 08:34 AM, FEBRUARY 5, 1999 01:33 PM...
TAG_INST_SW3	JANUARY 12, 1999 06:41 AM

SHARED SOFTWARE DATA SSD ACCESS TABLE

FIG. 14

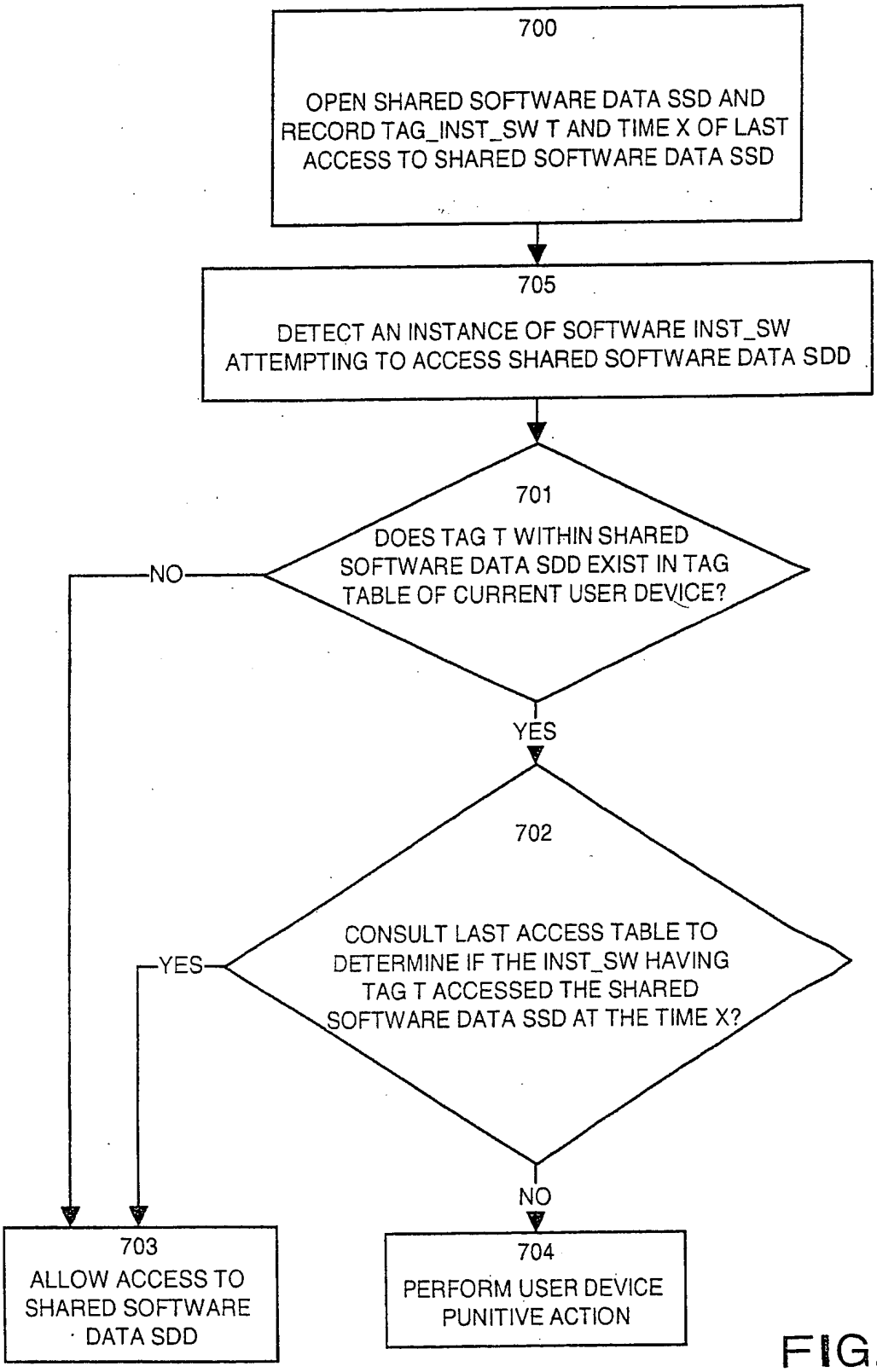

700
OPEN SHARED SOFTWARE DATA SSD AND RECORD TAG_INST_SW T AND TIME X OF LAST ACCESS TO SHARED SOFTWARE DATA SSD
705
DETECT AN INSTANCE OF SOFTWARE INST_SW ATTEMPTING TO ACCESS SHARED SOFTWARE DATA SDD
701
DOES TAG T WITHIN SHARED SOFTWARE DATA SDD EXIST IN TAG TABLE OF CURRENT USER DEVICE?
NO
YES
702
CONSULT LAST ACCESS TABLE TO DETERMINE IF THE INST_SW HAVING TAG T ACCESSED THE SHARED SOFTWARE DATA SSD AT THE TIME X?
YES
NO
703
ALLOW ACCESS TO SHARED SOFTWARE DATA SDD
704
PERFORM USER DEVICE PUNITIVE ACTION

FIG. 15